CLAIMS

What is claimed is:

1. A system for providing protection against malicious code, said system comprising:

a malicious code analyzer disposed in a communication system traffic pattern between an originator of an information communication of said communication system traffic pattern and an intended recipient of said information communication to intercept said information communication and to analyze said information communication for malicious code, said malicious code analyzer being configured to be transparent to systems of said communication system.

2. The system of claim 1, wherein said transparent configuration of said malicious code analyzer comprises said malicious code analyzer not having a network address associated therewith which is visible external to said system.

3. The system of claim 1, wherein said transparent configuration of said malicious code analyzer comprises:

a translate function that monitors each packet provided to an interface of said system for packets to be provided malicious code analysis by said malicious code analyzer.

4. The system of claim 1, wherein said malicious code analyzer comprises:

a proxy for emulating a behavior of a destination of said information communication.

5. The system of claim 4, wherein said transparent configuration of said malicious code analyzer renders said proxy invisible to devices coupled to said system.

6. The system of claim 4, wherein said proxy comprises:

server functionality; and

client functionality.

7. The system of claim 4, further comprising:

a loop back interface for interfacing said information communication with said malicious code analyzer.

8. The system of claim 1, wherein said malicious code analyzer comprises:

code for virus scanning.

9. The system of claim 1, wherein said malicious code analyzer comprises:

code for identifying unwanted or unsolicited messages.

10. The system of claim 1, further comprising:

a steering module for said information communication between a first interface and a second interface of said system, wherein said steering module provides a translate function that monitors each information communication provided to said first interface and said second interface for information communication to be provided malicious code analysis and directs at least some of said information communication to said malicious code analyzer.

11. The system of claim 1, further comprising:

a communications throttle for determining if said information communication is to be passed by said system.

12. The system of claim 1, wherein said information communication conforms to a protocol selected from the group consisting of:

simple mail transfer protocol (SMTP);

post office protocol (POP);

hypertext transfer protocol (HTTP);

Internet message access protocol (IMAP);

file transfer protocol (FTP);

domain name service (DNS);

hot standby router protocol (HSRP);

open shortest path first (OSPF); and

enhanced interior gateway routing protocol (EIGRP).

13. A computer program product having a computer readable medium having computer program logic recorded thereon for providing protection against malicious code, said computer program product comprising:

code for analyzing malicious code present in information communication traffic between an originator of an information communication of said communication traffic and an intended recipient of said information communication; and

code for a steering said information communication between interfaces associated with said information communication originator and said intended recipient and providing a translate function which detours at least a portion of said information communication to said code for analyzing malicious code and which renders said code for analyzing malicious code invisible to said information communication originator and said intended recipient.

14. The computer program product of claim 13, further comprising:

proxy code interfacing said information communication with said code for analyzing malicious code.

15. The computer program product of claim 14, wherein said proxy code comprises server and client functionality.

16. The computer program product of claim 13, wherein said code for analyzing malicious code comprises virus scanning code.

17. The computer program product of claim 13, wherein said code for analyzing malicious code comprises undesired or unsolicited message identification code.

18. The computer program product of claim 13, wherein said translate function monitors each information communication provided to a first interface of said interfaces and a second interface of said interfaces for information communication to be provided malicious code analysis.

19. The computer program product of claim 13, further comprising:

code for throttling communications by receiving information with respect to information communication and determining if said information communication is to be passed by said interfaces.

20. A method for providing protection against malicious code, said method comprising:

intercepting packets in an information communication traffic pattern;

steering said packets between interfaces associated with an information communication originator and said intended recipient, said steering providing detouring of at least a portion of said packets to a malicious code analyzer; and

analyzing said at least a portion of said packets by said malicious code analyzer before releasing said at least a portion of said packets back into said traffic pattern.

21. The method of claim 20, further comprising:

disposing a protective system providing said intercepting, steering, and analyzing in a network link between said information communication originator and said intended recipient.

22. The method of claim 21, wherein said protective system is disposed as a protected network edge device.

23. The method of claim 20, wherein said steering is accomplished in a manner which renders said malicious code analyzer invisible to said information communication originator and said intended recipient.

24. The method of claim 20, further comprising:

interfacing said information communication with said code for analyzing malicious code using a proxy.

25. The method of claim 21, wherein said proxy comprises a proxy server and a proxy client.

26. The method of claim 20, wherein said analyzing said at lest a portion of said packets comprises:

scanning for viruses.

27. The method of claim 20, wherein said analyzing said at least a portion of said packets comprises:

identifying undesired or unsolicited messages.

28. The method of claim 20, wherein said steering comprises:

monitoring each packet provided to a first interface and a second interface for information communication to be provided malicious code analysis.

29. The method of claim 20, further comprising:

throttling communications by receiving information with respect to said packets and determining if said packets are to be passed in said traffic pattern.

30. A system for providing protection against malicious code, said system comprising:

a steering module for directing packets between a first interface and a second interface of said system, wherein said steering module provides a translate function that monitors each packet provided to said first interface and said second interface for packets to be provided malicious code analysis and directs at least some of said packets to a malicious code analyzer; and

said malicious code analyzer coupled to said steering module for receiving packets which are not addressed for receipt by said malicious code analyzer but which are directed to said malicious code analyzer by said steering module and for providing packets analyzed by said malicious code analyzer to said steering module, wherein said malicious code analyzer provides a malicious code remediation function.

31. The system of claim 30, wherein said first interface is coupled to a network protected by said system and said second interface is coupled to a network not protected by said system.

32. The system of claim 31, wherein said system is disposed at an edge of said protected network.

33. The system of claim 30, wherein said steering module comprises:

a frame store storing packets as received by said first interface and said second interface.

34. The system of claim 30, wherein said steering module comprises:

a station map providing information with respect to which of said first interface and said second interface particular destinations of said packets are coupled to.

35. The system of claim 30, wherein said malicious code analyzer comprises:

a proxy for emulating a behavior of a destination of ones of said packets.

36. The system of claim 35, wherein said translate function of said steering module renders said proxy invisible to devices coupled to said first interface and said second interface.

37. The system of claim 35, wherein said proxy comprises:

a proxy server; and

a proxy client.

38. The system of claim 35, wherein said proxy communicates with said steering module using a network stack.

39. The system of claim 38, wherein said proxy communicates with said steering module using said network stack through use of a loop back interface.

40. The system of claim 30, wherein said malicious code analyzer comprises:

code for virus scanning.

41. The system of claim 40, wherein said code for virus scanning comprises:

commercially available virus scanning software integrated into said malicious code analyzer.

42. The system of claim 30, wherein said malicious code analyzer comprises:

code for identifying unwanted or unsolicited messages.

43. The system of claim 30, further comprising:

a communications throttle coupled to said steering module for receiving information with respect to packets which are not addressed for receipt by said communications throttle but which information with respect thereto is directed to said communications throttle by said steering module and for determining if said packets are to be passed by said system.